

10/13/00  
JC953 U.S. PTO

10-16-00

PTO  
10/13/00  
JC953 U.S. PTO  
10/13/00

Please type a plus sign (+) inside this box → ☒

PTO/SB/05 (4/98)  
Approved for use through 09/30/2000. OMB 0651-0032  
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE  
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

<b>UTILITY PATENT APPLICATION TRANSMITTAL</b> <small>(Only for new nonprovisional applications under 37 C.F.R. § 1.53(b))</small>	Attorney Docket No.	155638-0034
	First Inventor or Application Identifier	William S. Holmes
	Title	Method and Apparatus for Providing Verifiable Digital ...
	Express Mail Label No.	EL489787627US

APPLICATION ELEMENTS <small>See MPEP chapter 600 concerning utility patent application contents.</small>	ADDRESS TO: Assistant Commissioner for Patents Box Patent Application Washington, DC 20231
1. <input checked="" type="checkbox"/> * Fee Transmittal Form (e.g., PTO/SB/17) <small>(Submit an original and a duplicate for fee processing)</small>	5. <input type="checkbox"/> Microfiche Computer Program (Appendix)
2. <input checked="" type="checkbox"/> Specification [Total Pages <b>27</b> ] <small>(preferred arrangement set forth below)</small> <ul style="list-style-type: none"><li>- Descriptive title of the Invention</li><li>- Cross References to Related Applications</li><li>- Statement Regarding Fed sponsored R &amp; D</li><li>- Reference to Microfiche Appendix</li><li>- Background of the Invention</li><li>- Brief Summary of the Invention</li><li>- Brief Description of the Drawings (if filed)</li><li>- Detailed Description</li><li>- Claim(s)</li><li>- Abstract of the Disclosure</li></ul>	6. Nucleotide and/or Amino Acid Sequence Submission <small>(if applicable, all necessary)</small> <ul style="list-style-type: none"><li>a. <input type="checkbox"/> Computer Readable Copy</li><li>b. <input type="checkbox"/> Paper Copy (identical to computer copy)</li><li>c. <input type="checkbox"/> Statement verifying identity of above copies</li></ul>
3. <input checked="" type="checkbox"/> Drawing(s) (35 U.S.C. 113) [Total Sheets <b>6</b> ]	<b>ACCOMPANYING APPLICATION PARTS</b> 7. <input checked="" type="checkbox"/> Assignment Papers (cover sheet & document(s)) 8. <input type="checkbox"/> 37 C.F.R. § 3.73(b) Statement <input type="checkbox"/> Power of Attorney <small>(when there is an assignee)</small> 9. <input type="checkbox"/> English Translation Document (if applicable) 10. <input type="checkbox"/> Information Disclosure Statement (IDS)/PTO-1449 <input type="checkbox"/> Copies of IDS Citations 11. <input type="checkbox"/> Preliminary Amendment 12. <input checked="" type="checkbox"/> Return Receipt Postcard (MPEP 503) <small>(Should be specifically itemized)</small> 13. <input checked="" type="checkbox"/> * Small Entity Statement(s) <input type="checkbox"/> Statement filed in prior application, Status still proper and desired <small>(PTO/SB/09-12)</small> 14. <input type="checkbox"/> Certified Copy of Priority Document(s) <small>(if foreign priority is claimed)</small> 15. <input type="checkbox"/> Other: .....
4. Oath or Declaration [Total Pages <b>2</b> ] <ul style="list-style-type: none"><li>a. <input checked="" type="checkbox"/> Newly executed (original or copy)</li><li>b. <input type="checkbox"/> Copy from a prior application (37 C.F.R. § 1.63(d)) <small>(for continuation/divisional with Box 16 completed)</small><ul style="list-style-type: none"><li>i. <input type="checkbox"/> <b>DELETION OF INVENTOR(S)</b> Signed statement attached deleting inventor(s) named in the prior application, see 37 C.F.R. §§ 1.63(d)(2) and 1.33(b).</li></ul></li></ul>	
<b>* NOTE FOR ITEMS 1 &amp; 13: IN ORDER TO BE ENTITLED TO PAY SMALL ENTITY FEES, A SMALL ENTITY STATEMENT IS REQUIRED (37 C.F.R. § 1.27), EXCEPT IF ONE FILED IN A PRIOR APPLICATION IS RELIED UPON (37 C.F.R. § 1.28).</b>	

16. If a CONTINUING APPLICATION, check appropriate box, and supply the requisite information below and in a preliminary amendment:  
☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No: \_\_\_\_\_ / \_\_\_\_\_  
Prior application information: Examiner \_\_\_\_\_ Group / Art Unit: \_\_\_\_\_  
**For CONTINUATION or DIVISIONAL APPS only:** The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 4b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

<b>17. CORRESPONDENCE ADDRESS</b>					
<input type="checkbox"/> Customer Number or Bar Code Label (Insert Customer No. or Attach bar code label here) or <input checked="" type="checkbox"/> Correspondence address below					
Name	Babak Redjaian, Reg. No. 42,096				
	IRELL & MANELLA LLP				
Address	840 Newport Center Drive Suite 400				
City	Newport Beach	State	CA	Zip Code	92660
Country	USA	Telephone	(949) 760-0991	Fax	(949) 760-5200

Name (Print/Type)	Babak Redjaian	Registration No. (Attorney/Agent)	42,096
Signature	<i>Babak Redjaian</i>	Date	October 13, 2000

Burden Hour Statement: This form is estimated to take 4.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Approved for use through 09/30/2000. OMB 0651-0032  
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

PTO/SB/17 (12/99)

# FEE TRANSMITTAL for FY 2000

Patent fees are subject to annual revision.  
Small Entity payments must be supported by a small entity statement,  
otherwise large entity fees must be paid. See Forms PTO/SB/09-12.  
See 37 C.F.R. §§ 1.27 and 1.28.

TOTAL AMOUNT OF PAYMENT (\$ \$471.00

## Complete if Known

Application Number  
Filing Date  
First Named Inventor William S. Holmes  
Examiner Name  
Group / Art Unit  
Attorney Docket No. 155638-0034

## METHOD OF PAYMENT (check one)

1. ☒ The Commissioner is hereby authorized to charge indicated fees and credit any overpayments to:

Deposit Account Number 09-0946

Deposit Account Name Irell & Manella LLP

☒ Charge Any Additional Fee Required  
Under 37 CFR §§ 1.16 and 1.17

2. ☒ Payment Enclosed:  
☒ Check ☐ Money Order ☐ Other

## FEE CALCULATION

### 1. BASIC FILING FEE

Large Entity Fee Code (\$)	Small Entity Fee Code (\$)	Fee Description	Fee Paid
101 690	201 345	Utility filing fee	355
106 310	206 155	Design filing fee	
107 480	207 240	Plant filing fee	
108 690	208 345	Reissue filing fee	
114 150	214 75	Provisional filing fee	

SUBTOTAL (1) (\$ 355.00

### 2. EXTRA CLAIM FEES

Current	Pd	Prev	Extra	Fee from below	Fee Paid
Total Claims	24	20	4	9	36
Independent Claims	4	3	1	40	40
Multiple Dependent					

\*\*or number previously paid, if greater; For Reissues, see below

Large Entity Fee Code (\$)	Small Entity Fee Code (\$)	Fee Description
103 18	203 9	Claims in excess of 20
102 78	202 39	Independent claims in excess of 3
104 260	204 130	Multiple dependent claim, if not paid
109 78	209 39	** Reissue independent claims over original patent
110 18	210 9	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) (\$ 76.00

## FEE CALCULATION (continued)

### 3. ADDITIONAL FEES

Large Entity Fee Code (\$)	Small Entity Fee Code (\$)	Fee Description	Fee Paid
105 130	205 65	Surcharge - late filing fee or oath	
127 50	227 25	Surcharge - late provisional filing fee or cover sheet	
139 130	139 130	Non-English specification	
147 2,520	147 2,520	For filing a request for reexamination	
112 920*	112 920*	Requesting publication of SIR prior to Examiner action	
113 1,840*	113 1,840*	Requesting publication of SIR after Examiner action	
115 110	215 55	Extension for reply within first month	
116 380	216 190	Extension for reply within second month	
117 870	217 435	Extension for reply within third month	
118 1,360	218 680	Extension for reply within fourth month	
128 1,850	228 925	Extension for reply within fifth month	
119 300	219 150	Notice of Appeal	
120 300	220 150	Filing a brief in support of an appeal	
121 260	221 130	Request for oral hearing	
138 1,510	138 1,510	Petition to institute a public use proceeding	
140 110	240 55	Petition to revive - unavoidable	
141 1,210	241 605	Petition to revive - unintentional	
142 1,210	242 605	Utility issue fee (or reissue)	
143 430	243 215	Design issue fee	
144 580	244 290	Plant issue fee	
122 130	122 130	Petitions to the Commissioner	
123 50	123 50	Petitions related to provisional applications	
126 240	126 240	Submission of Information Disclosure Stmt	
581 40	581 40	Recording each patent assignment per property (times number of properties)	40.00
146 690	246 345	Filing a submission after final rejection (37 CFR § 1.129(a))	
149 690	249 345	For each additional invention to be examined (37 CFR § 1.129(b))	

Other fee (specify) Additional copies

Other fee (specify)

\* Reduced by Basic Filing Fee Paid

SUBTOTAL (3) (\$ 40.00

## SUBMITTED BY

Name (Print/Type)	Registration No. (Attorney/Agent)	Telephone	Date
Babak Redjaian	42,096	(949) 760-0991	October 13, 2000
Signature	Babak Redj.		

## WARNING:

Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

09/687288  
10/13/00



UNITED STATES PATENT APPLICATION

FOR

**METHOD AND APPARATUS FOR PROVIDING VERIFIABLE  
DIGITAL SIGNATURES**

INVENTOR:

**WILLIAM S. HOLMES**

Prepared by:

IRELL & MANELLA LLP  
840 Newport Center Drive, Suite 400  
Newport Beach, CA 92660  
(949) 760-0991

09637288-101300

## BACKGROUND OF THE INVENTION

### 1. Field of the Invention

The present invention relates generally to security, and specifically, to verifiable digital signatures.

### 2. Description of the Related Art

With the advancement of technology, the Internet is becoming more and more an integral part of our personal and professional lives. The Internet is heavily depended on for transmitting and receiving messages and documents via electronic mail. In a setting where a document is a legally and binding contract, the recipient must determine the identity of the person sending the document, and whether that person is authorized to bind the entity that the person is representing to a legal contract. The recipient must also ensure that the sender cannot later deny agreeing to the content(s) of the document (typically referred to as non-repudiation). The sender may also want to rely on the document that is received by the recipient.

Digital signature technology was developed primarily to authenticate the signer of the document and to ensure that the document remains unchanged when viewed by a recipient. Digital signatures are based on public key infrastructure (PKI) technology and use a combination of hashing and encryption to "encapsulate" the document in a form that proves unequivocally who has sent the document and that the document is exactly the same as the original.

At first glance, it appears that digital signatures are watertight, but the problem arises from the fact that the electronic document (e.g., a ".doc" file created by Microsoft Word™) is in computer format and cannot be read by the individual without the use of a "viewer" or word processing program. Different "viewer" or word processing programs or even different releases of the same program may



Variable	Mean	SD	Min	Max
Age	34.5	10.2	21	55
Gender	1.2	0.4	1	2
Marital status	1.5	0.5	1	3
Education	12.5	1.5	9	16
Income	1.8	0.8	1	3
Occupation	1.5	0.5	1	3
Religion	1.2	0.4	1	2
Health status	1.5	0.5	1	3
Stress level	2.5	1.0	1	4
Life satisfaction	3.5	1.0	1	5
Resilience	4.5	1.0	1	5
Optimism	3.5	1.0	1	5
Gratitude	3.5	1.0	1	5
Forgiveness	3.5	1.0	1	5
Empathy	3.5	1.0	1	5
Compassion	3.5	1.0	1	5
Kindness	3.5	1.0	1	5
Generosity	3.5	1.0	1	5
Patience	3.5	1.0	1	5
Humility	3.5	1.0	1	5
Modesty	3.5	1.0	1	5
Shyness	3.5	1.0	1	5
Introversion	3.5	1.0	1	5
Extroversion	3.5	1.0	1	5
Sensitivity	3.5	1.0	1	5
Emotionality	3.5	1.0	1	5
Neuroticism	3.5	1.0	1	5
Conscientiousness	3.5	1.0	1	5
Agreeableness	3.5	1.0	1	5
Openness	3.5	1.0	1	5
Stability	3.5	1.0	1	5
Control	3.5	1.0	1	5
Order	3.5	1.0	1	5
Discipline	3.5	1.0	1	5
Perseverance	3.5	1.0	1	5
Endurance	3.5	1.0	1	5
Stamina	3.5	1.0	1	5
Strength	3.5	1.0	1	5
Power	3.5	1.0	1	5
Influence	3.5	1.0	1	5
Authority	3.5	1.0	1	5
Leadership	3.5	1.0	1	5
Management	3.5	1.0	1	5
Organization	3.5	1.0	1	5
Planning	3.5	1.0	1	5
Execution	3.5	1.0	1	5
Completion	3.5	1.0	1	5
Success	3.5	1.0	1	5
Accomplishment	3.5	1.0	1	5
Achievement	3.5	1.0	1	5
Realization	3.5	1.0	1	5
Fulfillment	3.5	1.0	1	5
Satisfaction	3.5	1.0	1	5
Contentment	3.5	1.0	1	5
Peace	3.5	1.0	1	5
Harmony	3.5	1.0	1	5
Balance	3.5	1.0	1	5
Equilibrium	3.5	1.0	1	5
Stability	3.5	1.0	1	5
Consistency	3.5	1.0	1	5
Reliability	3.5	1.0	1	5
Trustworthiness	3.5	1.0	1	5
Credibility	3.5	1.0	1	5
Integrity	3.5	1.0	1	5
Honesty	3.5	1.0	1	5
Sincerity	3.5	1.0	1	5
Genuineness	3.5	1.0	1	5
Authenticity	3.5	1.0	1	5
Transparency	3.5	1.0	1	5
Openness	3.5	1.0	1	5
Accessibility	3.5	1.0	1	5
Approachability	3.5	1.0	1	5
Receptiveness	3.5	1.0	1	5
Open-mindedness	3.5	1.0	1	5
Flexibility	3.5	1.0	1	5
Adaptability	3.5	1.0	1	5
Resilience	3.5	1.0	1	5
Endurance	3.5	1.0	1	5
Stamina	3.5	1.0	1	5
Strength	3.5	1.0	1	5
Power	3.5	1.0	1	5
Influence	3.5	1.0	1	5
Authority	3.5	1.0	1	5
Leadership	3.5	1.0	1	5
Management	3.5	1.0	1	5
Organization	3.5	1.0	1	

5  
10

Other embodiments are described and claimed herein.

## BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 illustrates a block diagram of an exemplary system for transmitting and receiving electronic documents over a network in accordance with one or more embodiment(s) of the present invention.

5           Figure 2 illustrates a block diagram of a computer system, according to one embodiment of the present invention.

Figure 3 illustrates a logical block/flow diagram for creating a file archive on a computer system to be digitally signed, according to one embodiment of the present invention.

10           Figure 4 shows a file containing the trusted parameters, according to one embodiment of the present invention.

Figure 5 illustrates a logical block/flow diagram for digitally signing a file archive, according to one embodiment of the present invention.

15           Figure 6 illustrates a logical block/flow diagram on a receiver computer system, according to one embodiment of the present invention.



## DETAILED DESCRIPTION

The present invention comprises a method, apparatus, and computer readable program code for providing verifiable digital signatures. Consequently, the method and apparatus establishes integrity and trust in the digital signatures, providing evidence that the sending and receiving parties are seeing the identical view of the digitally signed document(s).

In one embodiment, a method includes converting, on a computer system, digital data representative of a document into a predetermined format, and applying the predetermined format and a viewer program to a hash function to mathematically operate on the predetermined format and the viewer program and provide a message digest. The viewer program is used for viewing the predetermined format that is a representation of the document. The method further includes encrypting the message digest using a private key to provide a digital signature. In one embodiment, the predetermined format is a bitmap representation of the document.

As discussed herein, a "computer" or "computer system" is a product including circuitry capable of processing data. The computer system may include, but is not limited to, a general purpose computer systems (e.g., server, laptop, desktop, palmtop, etc.), personal electronic devices (e.g., palm pilot), office equipment, banking equipment (e.g., an automated teller machine), electronic devices (e.g., CD/DVD player, receiver/tuner, television, etc.), cash registers, networked devices and appliances, and the like. A "communication link" is generally defined as any medium over which information may be transferred such as, for example, electrical wire, optical fiber, cable, plain old telephone system (POTS) lines, wireless (e.g., satellite, radio frequency "RF", infrared, etc.) and the like. A module may be implemented in software and/or hardware.

Figure 1 illustrates a block diagram of an exemplary system 100 for transmitting and receiving electronic documents over a network in accordance with one or more embodiment(s) of the present invention. Referring to Figure 1, the system 100 includes a sending party's ("sender") computer system 110 and a receiving party's ("receiver") computer system 115 coupled to a network cloud 120 via communication links 140 and 145, respectively. Each of the sender and receiver computer systems 110 and 115 includes a processor, memory, communication circuitry, etc. and software running thereon for digitally signing and verifying digitally signed documents according to the present invention. The sending computer system 110 is where an electronic document is created and/or digitally signed using the method and apparatus of the present invention, before transmission over the network cloud 120 to one or more recipients (e.g., a user at receiver computer system 115). On the receiver computer system 115, the digital signature is verified and the document is viewed and/or printed in accordance with the method and apparatus of the present invention.

The system optionally includes a viewer server 125 that is coupled to the network cloud 120 via communication link 150. The viewer server 125 is operated by a trusted third party that downloads, upon demand, an authorized viewer module to a receiver computer system for viewing documents, as will be described below in accordance with embodiments of the present invention. The server 125 may be an Internet portal that hosts web pages.

The system 100 further includes a sever 130 coupled to the network cloud 120 via communication link 155. In one embodiment, the server 130 downloads software programs and/or modules to the sender and/or receiving computer systems for implementing embodiments of the present invention, as will be described in more detail below. The server 130 may be an Internet portal including

web pages or other type of access point. The server 130 may be maintained, owned, and/or operated by a third party for facilitating the verifiable digital signature method and apparatus of the present invention. Note that viewer server 125 and server 130 may be merged into a single server and/or owned or operated by a common trusted third party.

Also included in the system 100 is an optional timestamp server 135, which may be maintained by an independent entity. The timestamp server 135 is coupled to the network cloud 120 via communication link 160. The timestamp server 135 is a trusted third party that digitally signs a digitally signed document to provide timestamp information to authenticate the time of the digital signature.

In one embodiment, the network cloud 120 includes a local area network (LAN), wide area network (WAN), Internet, other global computer network, Intranet, one or more direct link connections, and/or combinations thereof. For sake of clarity and to provide a non-restrictive example, the network cloud 120 will also be referred to herein as the Internet.

Figure 2 illustrates a block diagram of a computer system 200, according to one embodiment of the present invention. For sake of clarity, the computer system 200 is described with respect to the sender and/or receiver computer system 110 or 115 (Figure 1).

Referring to Figure 2, the computer system 200 includes a processor 210 that is coupled to a bus structure 215. The processor 210 may include a microprocessor such as a Pentium™ microprocessor, microcontroller, or any other of one or more devices that process data. Alternatively, the computer system 200 may include more than one processor. The bus structure 215 includes one or more buses and/or bus bridges that couple together the devices in the computer system 200.



viewer program, and/or trusted parameters, verify the digital signature, and verify that the environment for viewing the signed document is the same as the environment when the document was digitally signed, among other things.

The mass storage device 240 includes (but is not limited to) a hard disk, floppy disk, CD-ROM, DVD-ROM, tape, high density floppy, high capacity removable media, low capacity removable media, solid state memory device, etc., and combinations thereof. In one embodiment, the mass storage 240 is used to store documents, where digitally signed or not, a viewer program/module, etc. The mass storage may also store the operating system and/or modules that are loaded into system memory 220 at system startup.

The computer system 200 also includes a video controller 250 for driving a display device 255, one or more peripheral devices such as a printer, fax, etc., and a communication interface 270 such as a T1 connection for communicating over the network cloud 120 (Figure 1).

Also coupled to the bus structure 215 is an optional personal identification device 275 that includes a processor subsystem 280 and a card reader/writer 285, which may optionally include a keypad. The processor subsystem 280 includes a microprocessor or microcontroller, memory, and software running thereon for communicating with the card reader/writer 285 and other module(s) and/or devices in the computer system 200. In one embodiment, a user's private signing key and other information such as the user's personal information and PIN may be stored on a "smart" card 290, which includes a processor, memory, communication interface (e.g., serial interface), etc. Optionally, the personal identification device 275 or the card reader/writer 285 may include or may be coupled to one or more biometrics devices to scan in the user's thumb print, perform a retinal scan, and read

other biometrics information. In such a case, the "smart" card may include a digital representation of the user's thumb print, retinal scan, and the like.

When digitally signing documents or other objects, the user connects the "smart" card 290 to the card reader/writer 285 or some other location on the personal identification device 275 (e.g., via a serial port 295). Optionally, the keypad on the card reader/writer 285 may include a display that prompts the user to "Enter in a PIN" and/or "Provide biometrics authentication" (e.g., a thumb print). The PIN provided by the user is then uploaded to the "smart" card 290 via the serial port 295. The "smart" card then compares the PIN entered on the keypad and the PIN stored on the "smart" card. The "smart" card may also compare biometrics information (e.g., a user's thumb print) stored thereon with biometrics information scanned or otherwise obtained from the user. If there is a mismatch, the user may be prompted with a message such as "Incorrect PIN. Please Enter correct PIN". If they match, the "smart" card then requests the message digest (515, Figure 5) from the computer system for encrypting the message digest with the user's private signing key. The message digest 515 may be stored in system memory 220, mass storage 240, and/or other location. The message digest may be retrieved through the processor subsystem 280 or directly from the processor 210. In either case, the "smart" card 290 reads the message digest, and encrypts the same with the user's private signing key to provide a digital signature. The memory on the "smart" card 290 includes encryption algorithm and software for generating the digital signature based on the private key.

In another embodiment, the comparison of the PIN stored on the "smart" card 290 and the PIN entered by the user on the keypad, and the encryption of the message digest with the user's private signing key may be performed by the

processor subsystem 280. In such a case, the "smart" card downloads the PIN and the private signing key stored thereon to the processor subsystem 280.

Figure 3 illustrates a logical block/flow diagram 300 for creating a file archive on a computer system to be digitally signed, according to one embodiment of the present invention. Referring to Figure 3, a document 310 is created, stored, and/or loaded on a computer system (e.g., computer system 200 of Figure 2). The document 310 may comprise a datafile, letter, memorandum, note, other document such as a document having legal significance (e.g., contract), or combinations thereof, where it may be important to authenticate the signer of the document, and that both the signer and recipient view the identical document. For example, the document 310 may be a contract between two or more parties that is to be digitally signed by the parties to create an enforceable and binding agreement. The document 310 may be created as a ".doc", ".wp", or any other format (e.g., using a word processor program).

Once created and ready to be digitally signed, the document 310 is applied to a converter module 315 which converts the document 310 into a predetermined format that can be reconstructed to view the document. In the current embodiment, the predetermined format is a document bitmap 320 or bitmap representation of the document 310, though any other format may be used. The document bitmap 320 includes a bitmap body 325, and bitmap parameters 330 in a header. Such parameters include, but are not limited to, the protocol, version, formatting, etc. of the bitmap. In one embodiment, the converter module 315 is an application program, module, and/or driver (e.g., a printer driver) that works with many different applications or word processors to produce a standard bitmap graphical image of the document, which can be viewed or printed (e.g., similar to that produced by using a fax/print option). In another embodiment, the converter

module 315 may include a module that converts the format of the document 310 into formats such as ".gif", ".jpg", ".tiff", ".pdf", etc. Once converted, the document may be viewed, printed, and/or faxed in the converted format.

The document bitmap 320, a viewer module 340, and optionally a trusted parameters file 345 are packed, appended, and/or concatenated by a packer module 335. In one embodiment, the viewer module 340 is an application program for viewing, printing, faxing, etc. the document bitmap body 325 using the associated bitmap parameters 330. The viewer module 340 includes a viewer header that specifies how the resolution, color levels, compression, etc. are to be handled by the viewer module 340. In one embodiment, the viewer module 340 is an executable program ".exe". In another embodiment, the viewer module 340 is a driver or other program.

The trusted parameters 345 include information regarding the environment of the computer system when the document is digitally signed. The trusted parameters 345 include, but not limited to, the software and hardware configurations of the computer system when the document is digitally signed, thereby providing "trip wire" and tamper evidence measures. Other parameters include details of the production system used to generate the digitally signed document and the viewing standards necessary to review it. The trusted parameters allow for a representation of the exact conditions present at the time the digital signature occurs. The parameters are optional and expandable to include any type of information with respect to the digital signature.

By capturing a snapshot of the environment at the moment of the digital signature, an entity has more assurance in the verification of the signature.

Consequently, non-repudiation is more enforceable. The viewer also receives



further assurances that what the viewer is viewing is exactly what was intended to be signed.

Once packed, the packer module 335 produces a file archive 355. The file archive 355 includes the document bitmap 320, the viewer module 340, and/or the (optional) trusted parameters 345. The file archive 355 may further include a file header 350 (dashed lines) for adding many other components and in a specified file format that may be understood by the sender and receiver computer systems. Consequently, the layout of the file archive 355 is exemplary, and may vary.

The process or technique of creating the file archive 355 may be implemented by one or more module(s) (either in software or hardware). In the case of a software module, such module may be downloaded from a third party entity (e.g., server 130 of Figure 1) over the Internet.

Figure 4 shows a file 400 containing the trusted parameters 345, according to one embodiment of the present invention. Referring to Figure 4, the file 400 includes an optional version number field 410 specifying the format or protocol of the parameters, optional server supplied viewer field 415, optional receiver computer system viewer field 420, sending computer system hardware information field 425, sending computer system software information field 430, and signature subsystem field 435.

The server computer system viewer field 415 is utilized when the viewer module is not included in the file archive 355 (Figure 3), but is downloaded from a remote server (e.g., viewer server 125, Figure 1) coupled to the network cloud 120. Thus, the signor of the document can specify in this field the version, number, and other identifier to allow the recipient(s) to download the correct viewer from the remote server for viewing the document bitmap, which is representative of the

document. The receiver computer system viewer field 420 is also utilized when the viewer module is not included in the file archive 355, but is located on the recipient's computer system, or may be obtained and loaded on the recipient's computer system. These fields specify the version, number, and other identifier of the viewer module to be used for viewing the document on the recipient's computer system. For example, these fields may include that the viewer used to sign the document is Microsoft™ Word™ xx-yyyy, version zz, where "xx-yyyy" is the month and year of release, and "zz" is the version number.

The hardware information field 425 specifies the hardware environment of the sender computer system at the time of signing. The field includes, but is not limited to, the video card and monitor type, version, etc. at the time of signing, and other tamper evidence measures. The software information field 430 specifies the software environment on the sender computer system at the time of signing. The field 430 includes, but is not limited to, the operating system, version of the operating system, tripwire information, applications and virtual machines, video software name and version, signing interface library (SIL) type and version, etc. In one embodiment, the virtual machine identifies the minimum number of components necessary to view the document.

The signature subsystem field 435 includes the token type such as "smart" card, PCMCIA card, button, dongle, etc., the reader/writer information (version, type, etc.), and other authentication information to the token. Such authentication may include PIN pad information, protected PIN path information, and one or more biometrics authentication information. The PIN pad information specifies keypad information such as the type, version, etc. The protected PIN path information specifies path of the PIN entered on the keypad. For example, if the keypad is directly coupled to the "smart" card, then the PIN may be sent to the "smart" card



operating the timestamp server 135, Figure 1) for including a digital timestamp signature 535 to the document 540. The timestamp signature 535, in addition to including the time of the timestamp signature, may include the trusted time entity and other information. In one embodiment, the document 540 is transmitted over the Internet to the timestamp server 135 (Figure 1), and sent back to the sender for transmission to the recipient(s). Alternatively, the timestamp server 130 digitally signs the document 540 with timestamp information and directly transmits the "timestamped" document 540 to the recipient(s).

Figure 6 illustrates a logical block/flow diagram of a module 600 on a receiver computer system, according to one embodiment of the present invention. The receiver computer system receives (e.g., over the Internet) or loads (e.g., from a disk) the digitally signed document 540. The file archive 355 and digital signature 530 may also be stored on mass storage 240 (Figure 2).

Referring to Figure 6, if the document 540 includes a timestamp signature 535, the timestamp information is verified. The file archive 355 is applied to an unpacker module 640 which unpacks the file archive 355 into the document bitmap 645 (and/or optionally the original document), the viewer module 650, if included, and the trusted parameters 655, if packed in the file archive 355. The trusted parameters may also be obtained from the digital signature 530. Additionally, the digital signature 530 is applied to a signature function 610. Using the sender's public key 615, the digital signature 530 is decrypted, and the output is the message digest 620. The file archive 355 is also applied to a hash function 630, either before or after operation of the signature function 610, which operates on the file archive 355, using the same hash algorithm as used on the sending computer system, to yield a (calculated) message digest 635.

006107" 8836350

The (calculated) message digest 635 is then compared with the (received) message digest 620 to determine the integrity of the digital signature. If the two files are unequal, then the digital signature is not valid, and authentication cannot be confirmed. A message may be sent to a monitor stating that the digital signature is not valid. Consequently, viewing of the document may be disallowed. The receiver computer system may optionally send a message back to the sender computer system to notify the same of the mismatch.

If the two message digests are identical, the trusted parameters 655 may be examined to determine whether the receiver's computer system includes the same environment as the sender's computer system, when the document was digitally signed. In particular, the module 600 verifies the components of the computer system including the video card, monitor, other tamper evidence measures, operating system, applications, virtual machines, video software, etc. (as specified in fields 425 and 430, Figure 4). If the module 600 encounters any software, hardware, virtual machine, video subsystem, etc. that it does not understand and/or trust, the module reports a warning and may not show the document. The module 600 may then create a new file (not shown) including the original file archive and information regarding the viewing environment (e.g., error points).

However, if the viewing environment is the same as the signing environment, then the module 600 executes the viewer module 650 to view the document bitmap 645.

The present invention may be implemented as a method, apparatus, system, etc. When implemented in software, the elements of the present invention are essentially the code segments to perform the necessary tasks. The program or code segments can be stored in a processor readable medium or transmitted by a computer data signal embodied in a carrier wave over a transmission medium or

communication link. The "processor readable medium" may include any medium that can store or transfer information. Examples of the processor readable medium include an electronic circuit, a semiconductor memory device, a ROM, a flash memory, an erasable ROM (EROM), a floppy diskette, a CD-ROM, an optical disk, a  
5 hard disk, a fiber optic medium, a radio frequency (RF) link, etc. The computer data signal may include any signal that can propagate over a transmission medium such as electronic network channels, optical fibers, air, electromagnetic, RF links, etc.

While certain exemplary embodiments have been described and shown in the accompanying drawings, it is to be understood that such embodiments are merely  
10 illustrative of and not restrictive on the broad invention, and that this invention not be limited to the specific constructions and arrangements shown and described, since various other modifications may occur to those ordinarily skilled in the art.

## CLAIMS

What is claimed is:

1           1.       A digital signature method, comprising:  
2           converting, on a computer system, digital data representative of a document  
3 into a predetermined format;  
4           applying the predetermined format and a viewer program to a hash function  
5 to mathematically operate on the predetermined format and the viewer program  
6 and provide a message digest, the viewer program for viewing the predetermined  
7 format that is a representation of the document; and  
8           encrypting the message digest using a private key to provide a digital  
9 signature.

1           2.       The digital signature method of claim 1, further comprising  
2 incorporating into the digital signature a file including one or more parameters  
3 specifying an environment of the computer system at the time of creation of the  
4 digital signature.

1           3.       The digital signature method of claim 2, wherein said one or more  
2 parameters includes one or both of a type and version of one or more of the  
3 following: a video card, monitor, operating system, application program, and  
4 signing interface library of the computer system.









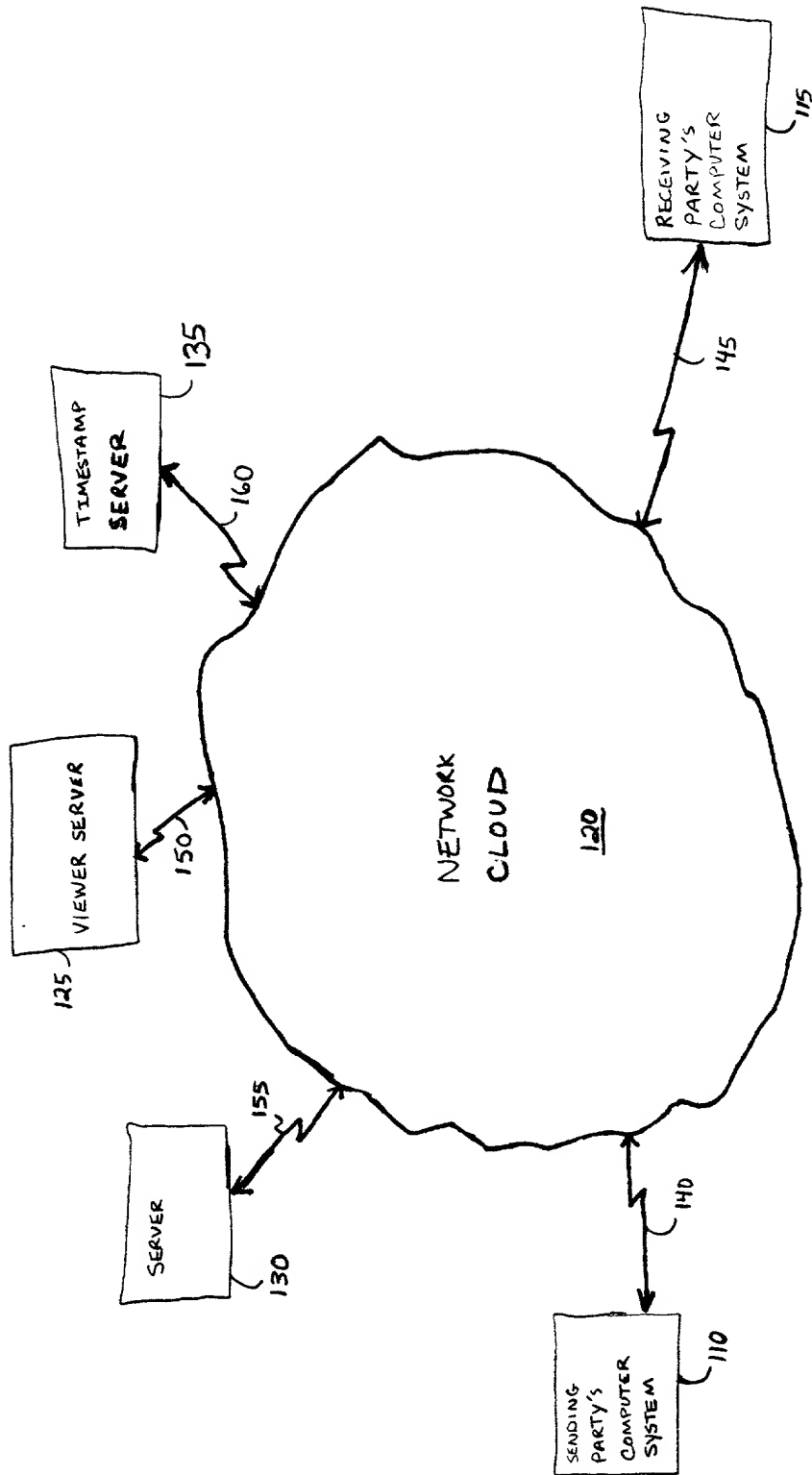






## ABSTRACT

A method and apparatus for providing verifiable digital signatures. In one embodiment, a method includes converting, on a computer system, digital data representative of a document into a predetermined format, and applying the predetermined format and a viewer program to a hash function to mathematically operate on the predetermined format and the viewer program and provide a message digest. The viewer program is used for viewing the predetermined format that is a representation of the document. The method further includes encrypting the message digest using a private key to provide a digital signature. In one embodiment, the predetermined format is a bitmap representation of the document. Moreover, in one embodiment, the method further includes incorporating a file in the digital signature, where the file includes one or more parameters specifying an environment of the computer system at the time of creation of the digital signature. The method and apparatus establishes integrity and trust in digital signatures, providing evidence that the sending and receiving parties are seeing the identical view of the digitally signed document(s).



100  
Figure 1

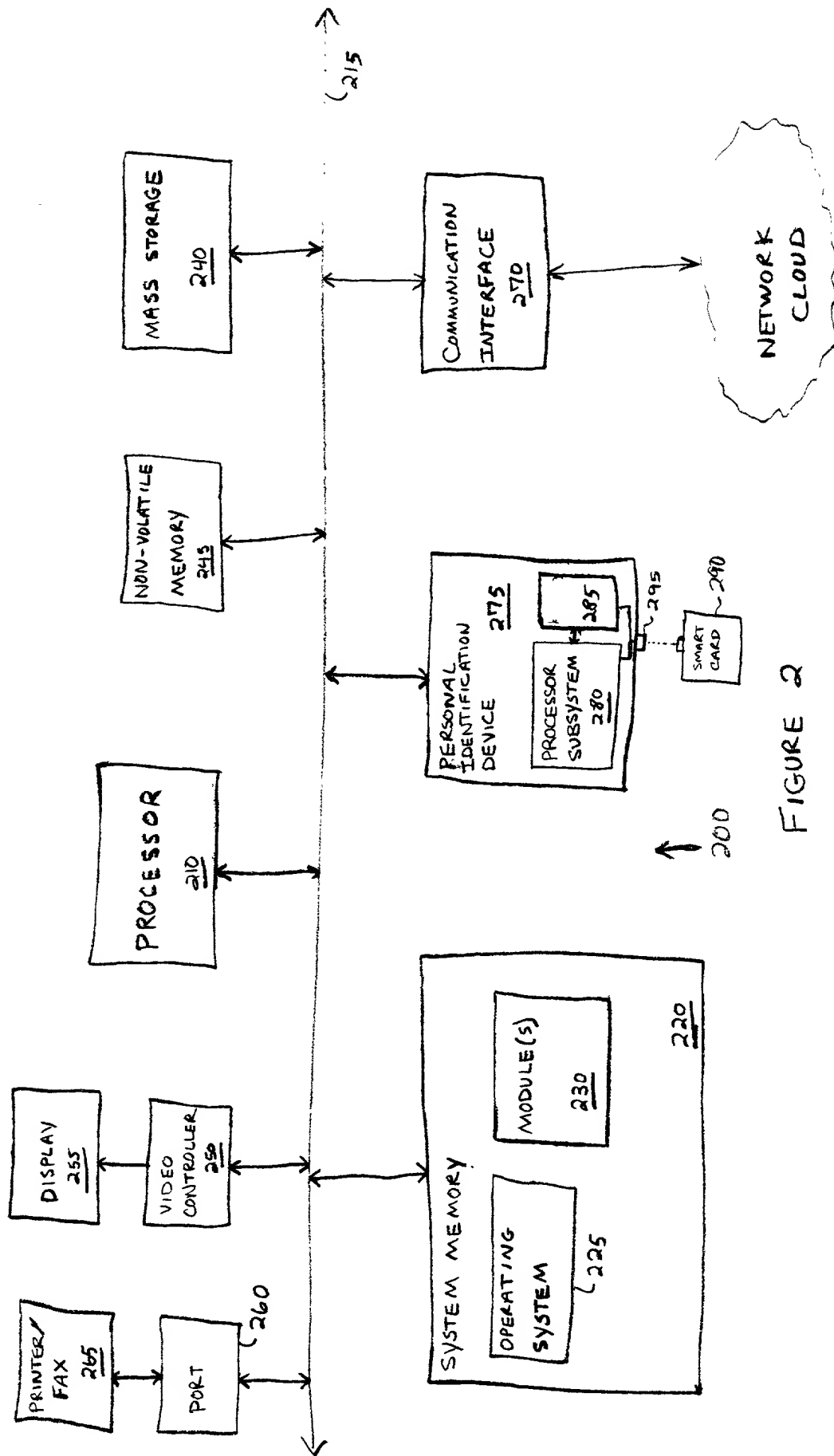


FIGURE 2



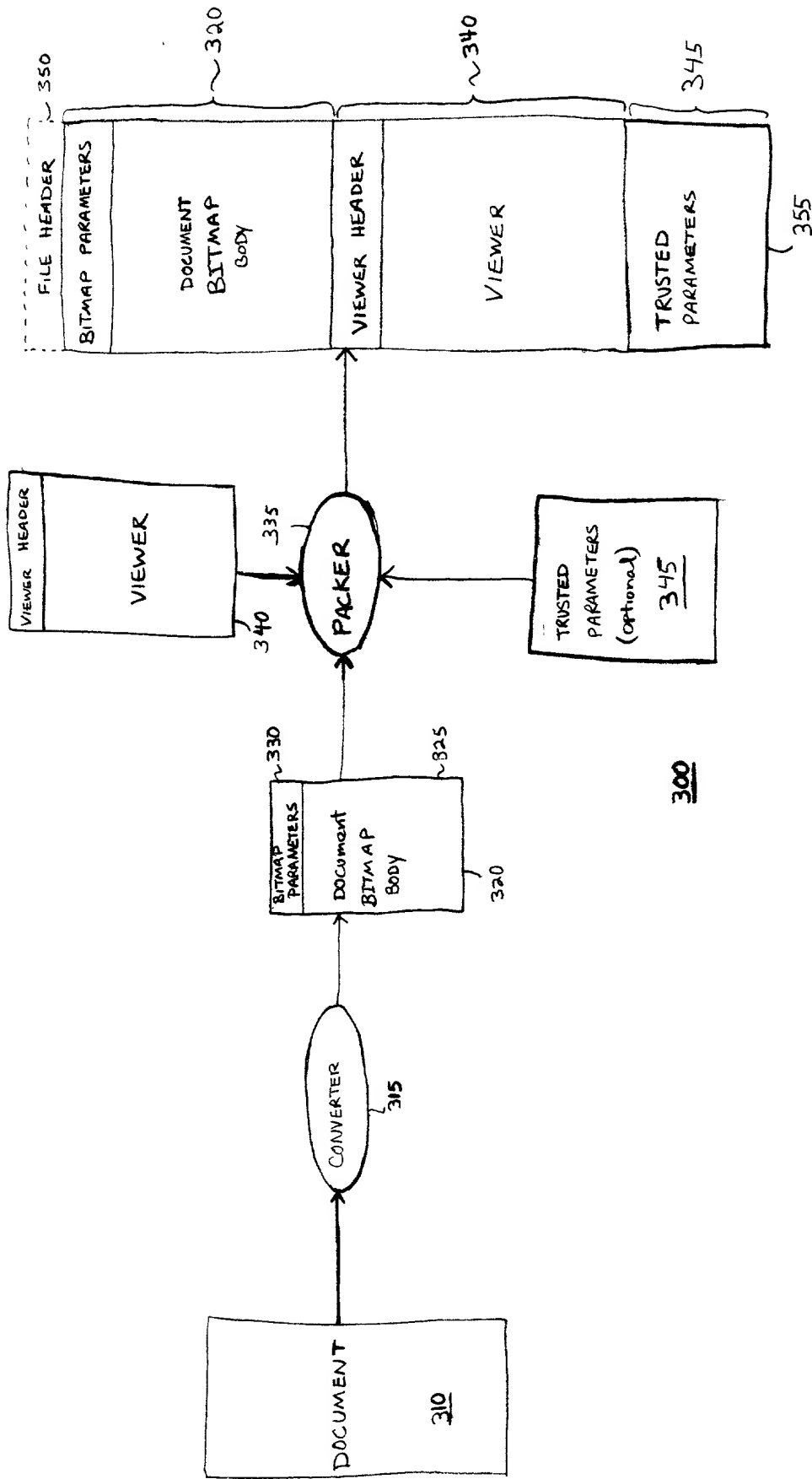
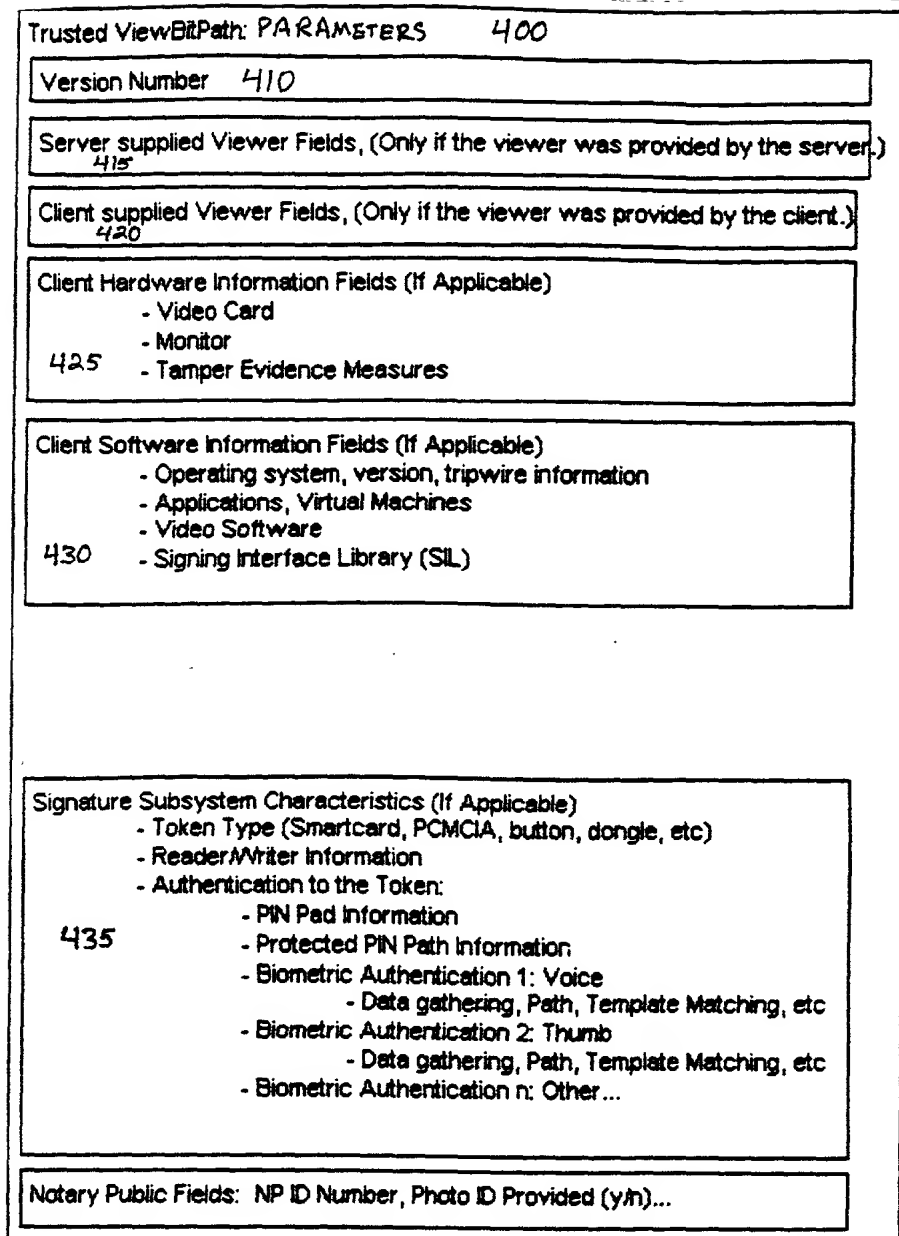


Figure 3



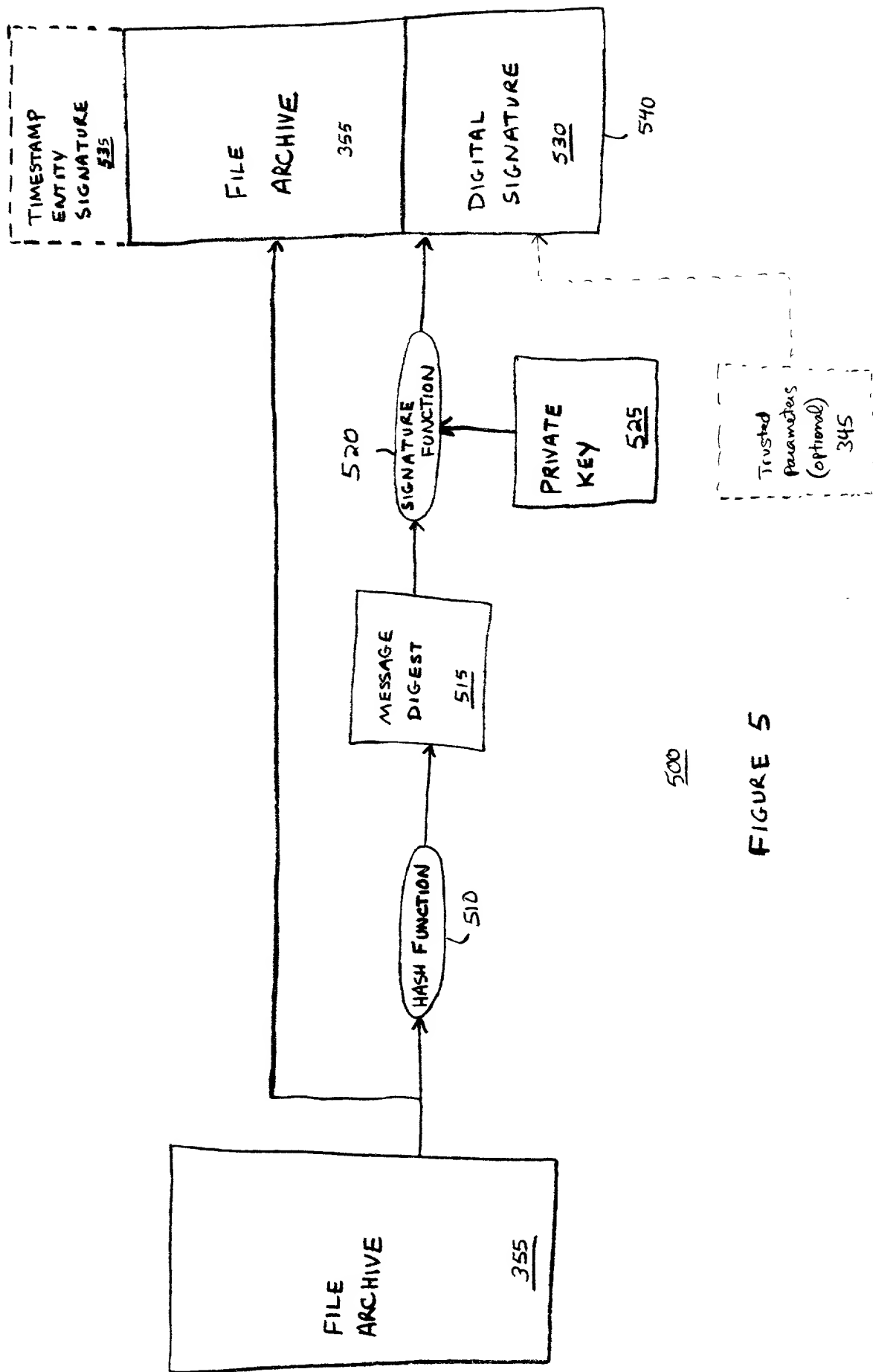
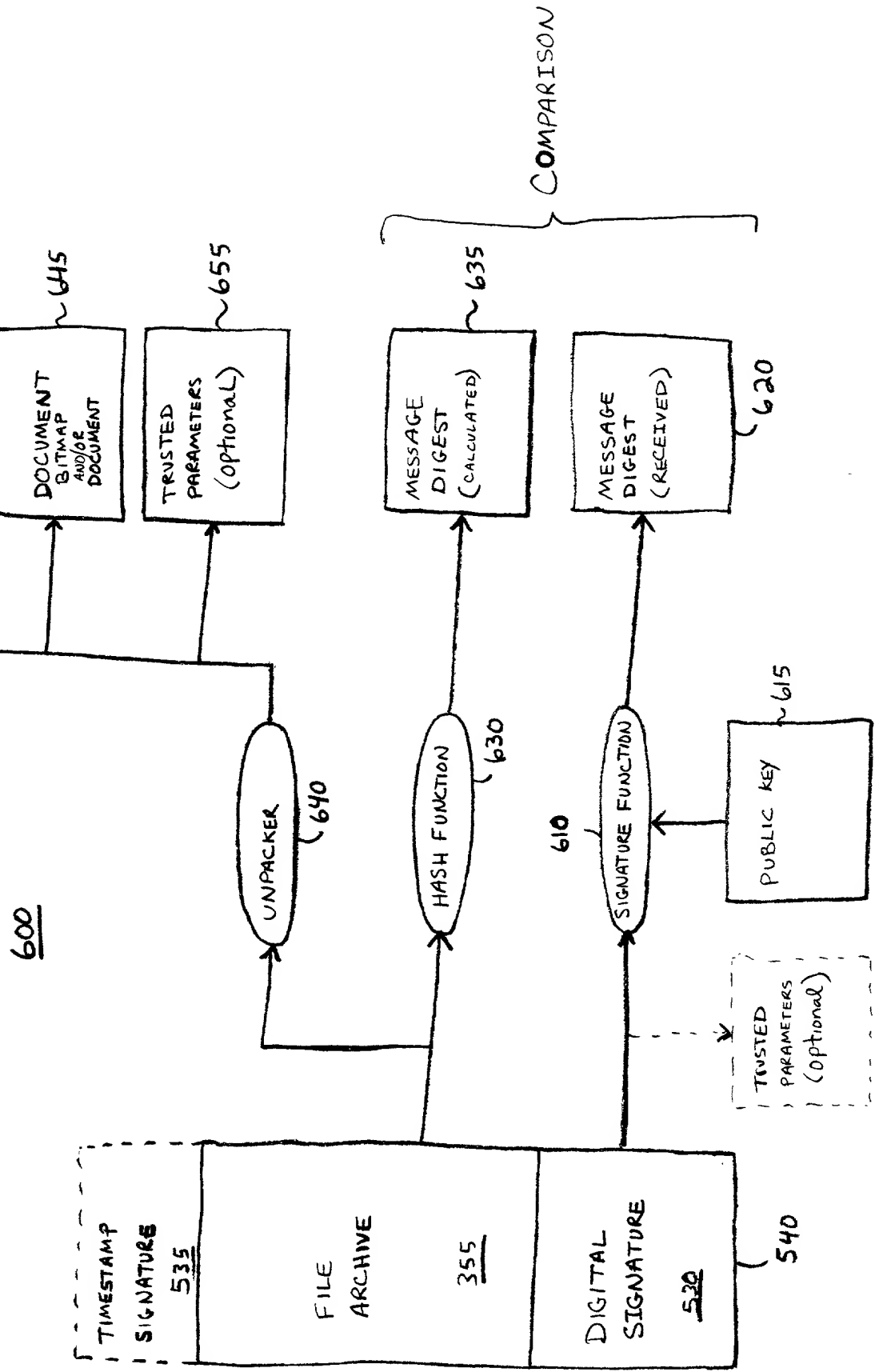


FIGURE 5

FIGURE 6



**DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION**

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below, next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or any original, first, and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

# METHOD AND APPARATUS FOR PROVIDING VERIFIABLE DIGITAL SIGNATURES

the specification of which

☒

is attached hereto.

11

was filed on \_\_\_\_\_ as

United States Application Number

or PCT International Application Number

and was amended on

(if applicable)

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claim(s), as amended by any amendment referred to above. I do not know and do not believe that the claimed invention was ever known or used in the United States of America before my invention thereof, or patented or described in any printed publication in any country before my invention thereof or more than one year prior to this application, that the invention was not published in an application filed before my invention, that the same was not in public use or on sale in the United States of America more than one year prior to this application, and that the invention has not been patented or made the subject of an inventor's certificate issued before the date of this application in any country foreign to the United States of America on an application filed by me or my legal representatives or assigns more than twelve months (for a utility patent application) or six months (for a design patent application) prior to this application.

I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d), of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s);

APPLICATION NUMBER	COUNTRY (OR INDICATE IF PCT)	DATE OF FILING (day, month, year)	PRIORITY CLAIMED UNDER 35 USC 119 <input type="checkbox"/> No <input type="checkbox"/> Yes

I hereby claim the benefit under Title 35, United States Code, Section 119(e) of any United States provisional application(s) listed below:

APPLICATION NUMBER	FILING DATE

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

APPLICATION NUMBER	FILING DATE	STATUS (ISSUED, PENDING, ABANDONED)

I hereby appoint IRELL & MANELLA LLP, a firm including: Paul Backofen, Reg. No. 42,278; Norman E. Brunell, Reg. No. 26,533; Douglas Carsten, Reg. No. 43,534; Gary Frischling, Reg. No. 35,515; Benjamin Hattenbach, Reg. No. 41,820; Andrei Iancu, Reg. No. 41,862; Soyeon Pak Laub, Reg. No. 39,266; Samuel K. Lu, Reg. No. 40,707; Kimberley G. Nobles, Reg. No. 38,255; Lisa Partain, Reg. No. 40,763; Babak Redjaian, Reg. No. 42,096; Flavio Rose, Reg. No. 40,791; David Rosman, Reg. No. 43,059; Peter Wied, Reg. No. 43,264; Sharon Wong, Reg. No. 37,760; and Ben J. Yorks, Reg. No. 33,609; my attorneys; with offices located at 840 Newport Center Drive, Suite 400, Newport Beach, California 92660, telephone (949) 760-0991, with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.

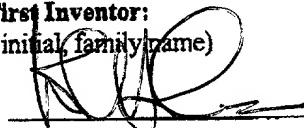
I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

**Full Name of Sole/First Inventor:**

(given name, middle initial, family name)

William S. Holmes

Inventor's Signature



Date

7/28/00

Residence

Santa Ana, CA  
(City, State)

Citizenship

United Kingdom

P.O. Address

11162 Wickford Drive  
Santa Ana, CA 92705**Full Name of Second/Joint Inventor:**

(given name, middle initial, family name)

Inventor's Signature

Date

Residence

(City, State)

Citizenship

(Country)

P.O. Address